SW

UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/517,608	03/02/2000	Simon Robert Walmsley	AUTH10US	4148

7590 10/07/2003	EXAMINER
Kia Silverbrook	NGUYEN, NGA B

Kia Silverbrook
Silverbrook Research Pty Ltd
393 Darling Street
Balmain,   2041
AUSTRALIA

ART UNIT	PAPER NUMBER
3628	

DATE MAILED: 10/07/2003

Please find below and/or attached an Office communication concerning this application or proceeding.

PTO-90C (Rev. 10/03)

-- The MAILING DATE of this communication appears on the c ver sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE <u>3</u> MONTH(S) FROM
THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed
  after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any
  earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on <u>02 March 2000</u> .

2a)☐ This action is **FINAL**.   2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is
closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) <u>1-27</u> is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) <u>1-27</u> is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

11)☐ The proposed drawing correction filed on _____ is: a)☐ approved b)☐ disapproved by the Examiner.

    If approved, corrected drawings are required in reply to this Office action.

12)☐ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. §§ 119 and 120

13)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a)☒ All b)☐ Some * c)☐ None of:

        1.☐ Certified copies of the priority documents have been received.

        2.☒ Certified copies of the priority documents have been received in Application No. <u>09/113,223</u> .

        3.☐ Copies of the certified copies of the priority documents have been received in this National Stage
           application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

14)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).

    a) ☐ The translation of the foreign language provisional application has been received.

15)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO-1449) Paper No(s) <u>2</u> .

4) ☐ Interview Summary (PTO-413) Paper No(s). _____ .

5) ☐ Notice of Informal Patent Application (PTO-152)

6) ☐ Other: .

DETAILED ACTION

1.   This Office Action is the answer to the communication filed on March 2, 2000,

which paper has been placed of record in the file.

2.   Claims 1-27 are pending in this application.

Claim Objections

3.   Claims 14-27 are objected to under 37 CFR 1.75(c), as being of improper

dependent form for failing to further limit the subject matter of a previous claim.

Applicant is required to cancel the claim(s), or amend the claim(s) to place the claim(s)

in proper dependent form, or rewrite the claim(s) in independent form. A proper

dependent claim shall not conceivably be infringed by anything that would not also

infringe the base claim. See MPEP 608.01(n), Section III. The system claims 14-27

infringe the method steps of claims 1-13 because they recite the means which are used

to perform the method of claims 1-13 (a random number generator, an asymmetric

encryptor, an trusted authentication chip, a test function). As a result, claims 14-27 are

improper dependent claims.

Double Patenting

4.   The nonstatutory double patenting rejection is based on a judicially created

doctrine grounded in public policy (a policy reflected in the statute) so as to prevent the

unjustified or improper timewise extension of the "right to exclude" granted by a patent

and to prevent possible harassment by multiple assignees. See *In re Goodman*, 11

F.3d 1046, 29 USPQ2d 2010 (Fed. Cir. 1993); *In re Longi*, 759 F.2d 887, 225

USPQ 645 (Fed. Cir. 1985); *In re Van Ornum*, 686 F.2d 937, 214 USPQ 761 (CCPA

1982); *In re Vogel*, 422 F.2d 438, 164 USPQ 619 (CCPA 1970);and, *In re Thorington*,

418 F.2d 528, 163 USPQ 644 (CCPA 1969).

A timely filed terminal disclaimer in compliance with 37 CFR 1.321(c) may be

used to overcome an actual or provisional rejection based on a nonstatutory double

patenting ground provided the conflicting application or patent is shown to be commonly

owned with this application. See 37 CFR 1.130(b). Effective January 1, 1994, a

registered attorney or agent of record may sign a terminal disclaimer. A terminal

disclaimer signed by the assignee must fully comply with 37 CFR 3.73(b).

5.   Claims 1, 2, 11-15, 24, 25, 27 are rejected under the judicially created doctrine of

obviousness-type double patenting as being unpatentable over claims 1-4, 6, 7, 13-18

of U.S. Patent No. 6,374,354. Although the conflicting claims are not identical, they are

not patentably distinct from each other because claims 1-4, 6, 7, 13-18 of U.S. Patent

No. 6,374,354 discloses the consumable authentication protocol and system for

validating the authenticity of an untrusted authentication chip using a one-way function

(an asymmetric encryption function is a one-way function).

Claim Rejections - 35 USC § 102

6.   The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that

form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

7.   Claims 1-5, 8-11, 13-18, 21-24, and 27 are rejected under 35 U.S.C. 102(b) as being anticipated by Bjerrum et al (hereinafter Bjerrum), U.S. Patent No. 5,311,595.

Regarding to claim 1, Bjerrum discloses a consumable authentication protocol for validating the authenticity of an untrusted authentication chip (figure 1, second electronic card 224), the protocol includes the steps of:

generating a random number and applying an asymmetric encrypt function to the random number using a first key to produce a first outcome (column 4, lines 43-49 and column 25, line 25-column 26, line 7);

passing the first outcome to the untrusted authentication chip (column 4, lines 50-64);

decrypting the first outcome with an asymmetric decrypt function using a secret key to produce a second outcome, in the untrusted chip (column 4, line 65-column 5, line 8);

applying the asymmetric encrypt function to the second outcome together with a data message read from the untrusted chip using the secret key to produce a third outcome, in the untrusted chip (column 5, lines 8-27);

receiving the third outcome together with the data message (column 5, lines 28-40);

decrypting the third outcome and comparing the decrypted random number and data message with the generated random number and the receive data message (column 5, lines 41-57);

in the event of a match, considering the untrusted chip and the data message to

be valid (column 5, lines 58-68);

otherwise considering the untrusted chip and the data message to be invalid

(column 6, line 62-column 7, line 5).

Regarding to claim 2, Bjerrum discloses for validating the authenticity of an

untrusted authentication chip, as well as ensuring that the authentication chip, lasts only

as long as the consumable including the further steps of writing new data to the

untrusted chip, performing the steps of claim 1, and in the event the untrusted is found

to be authentic and the new data is the same as the data message read from the

untrusted chip, then the write is validated (column 5, lines 5-8).

Regarding to claim 3, Bjerrum discloses the first key is a public key (column 25,

lines 35-40).

Regarding to claim 4, Bjerrum discloses encryption outside the untrusted chip is

implemented in software (column 4, lines 44-49, encryption in the first electronic card,

and encryption algorithm is a software).

Regarding to claim 5, Bjerrum discloses the random number generation,

encryption, passing, and final decrypting and comparing steps take place in an external

system (column 5, lines 35-68, all steps take place in the first computer system).

Regarding to claim 8, Bjerrum discloses the encryption outside the untrusted chip

is implemented in a second authentication chip, and an external system intermediated

between the two chips (column 4, lines 44-56, the encryption is implement in the first

electronic card and first computer system is the external system).

Regarding to claim 9, Bjerrum discloses the second authentication chip and

system are in a printer or other device in which consumables are mounted (figure 1,

item 124).

Regarding to claim 10, Bjerrum discloses the untrusted chip is in the consumable

(figure 1, item 224).

Regarding to claim 11, Bjerrum discloses the secret key is held only by the

untrusted chip (column 25, lines 40-41).

Regarding to claim 13, Bjerrum does not teach the data message is a memory

vector of the authentication chip, a part is different for each chip, and parts of it are

constant (read only) for each consumable, or decrement only so that it can be

completely downcounted only once for each consumable (column 21, lines 10-53, chip

card contains read only memory and data memory).

Regarding to claim 14, Bjerrum discloses a consumable authentication system

includes:

a random number generator (column 25, lines 20-21);

an asymmetric encryptor to encrypt generated random number with an

asymmetric encryption function to produce a first outcome and a first key for the

encryptor (column 4, lines 44-49, encryption means);

a test function and an untrusted authentication chip includes a read function

which operates to decrypt the first outcome using a secret key and produce a second

outcome, then applies the symmetric encryption function to the second outcome to the

second outcome together with a data message read using the secret key to produce a

third outcome, it also returns the third outcome together with the data massage in the clear; the test function operates to decrypt the third outcome and compare the decrypted second outcome and data message with the generated random and the clear data message; in the event of match the test function returns a valued indicating validity; otherwise it returns a value indicating invalidity (column 5, lines 5-68).

Claims 15-18, 21-24, 27 contain similar limitations found in claims 2-5, 8-11, 13, discussed above, therefore are rejected by the same rationale.

Claim Rejections - 35 USC § 103

8.   The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

9.   Claims 6, 7, 12, 19, 20, 25, and 26 are rejected under 35 U.S.C. 103(a) as being unpatentable over Bjerrum et al (hereinafter Bjerrum), U.S. Patent No. 5,311,595.

Regarding to claims 6, 7, Bjerrum does not teach the external system is in a printer or other device in which consumables such as ink cartridges are mounted, and the untrusted chip is in the consumable. However, a printer or other devices in which consumables such as ink cartridges are mounted such as copy machine, camera, etc...are well known devices. Therefore, it would have been obvious to apply Bjerrum's cryptography method for those devices for the purpose of prevent the unauthorized person to use such devices.

Regarding to claims 12, 26, Bjerrum does not teach the trusted authentication chip contains a random function to produce random numbers from a seed, and the function advances after every successful authentication so that the next random number will be produced from a different seed, for a group of authentication chips, the initial seed for each chip is different from that of the others in the group so that the first random number produced by each chip in the group will be different. However, it is well known to generate the next random number using a different seed in order to improve the level of security, and to use a different initial seed for each chip in the group of chip. Therefore, it would have been obvious to modify Bjerrum's to include the feature above for the purpose of providing high security level because each next random number is generated from a different seed and each chip has a different initial seed, thus the unauthorized person cannot easily to predict the random number.

Claims 19, 20, 25 contain similar limitations found in claims 6, 7, 12, discussed above, therefore are rejected by the same rationale.

Conclusion

10.   Claims 1-27 are rejected.

11.   The prior arts made of record and not relied upon is considered pertinent to applicant's disclosure:

Ishii (US 5,768,389) discloses method and system for generation and management of secret key of public key cryptosystem.

Shin et al (US 5,987,134) discloses a device for authenticating user's access rights.

Broseghini et al (US 5,416,783) discloses method and apparatus for generating pseudo-random numbers.

Thomlinson et al (US 5,778,069) discloses a computer-imolented pseudo random number generator.

12.   Any inquiry concerning this communication or earlier communications from the examiner should be directed to examiner Nga B. Nguyen whose telephone number is (703) 306-2901. The examiner can normally be reached on Monday-Thursday from 9:00AM-6:00PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Hyung S. Sough can be reached on (703) 308-0505.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the Group receptionist whose telephone number is (703) 306-1113.

13.   Any response to this action should be mailed to:

Commissioner of Patents and Trademarks

C/o Technology Center 3600

Washington, DC 20231

Or faxed to:

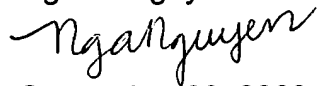(703) 872-926 (for formal communication intended for entry),

or

(703) 308-3691 (for informal or draft communication, please label

"PROPOSED" or "DRAFT").

Hand-delivered responses should be brought to Crystal Park 5, 2451 Crystal

Drive, Arlington, VA, Seventh Floor (Receptionist).

Nga B. Nguyen

September 30, 2003